Section III:	**Application Security**
Title:	**Information System Security Plan Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**June 5, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To assist North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices to develop and document an Information System Security Plan that provides important information about the system, the security requirements for the system and the security controls needed to meet the requirements.

STANDARD

1.0 Background

Today's rapidly changing technical environment and increasing vulnerabilities require organizations to adopt a minimum set of security controls to protect their data and information systems. Because of the potential for common security control interdependence by many of an organization's information systems, a failure of one such common control may result in a significant increase in the organizational level of risk—risk that arises from the operation of the system or systems that depend on these controls. The Information System Security Plan is intended to provide users and administrators with a thorough understanding of the system, the scope of use, and interconnectivity as well as general and specific vulnerabilities of the system. In addition, the plan outlines the controls that are planned for or implemented to guard against the loss of confidentiality, integrity, and availability of the information system or the data used, processed, stored, or transmitted by the system. System security planning is an important activity that supports the development of the NC DHHS Security Standards, Application Security - System Development Life Cycle Standard and should be updated as required to accurately reflect the most current state of the system.

2.0 Information System Identification

Each system for which a Division or Office is responsible shall be assigned a name and unique identifier to support the ability of the Division Information Security Official (ISO) to collect security metrics specific to the system as well as facilitate complete traceability of all requirements related to system implementation and performance. This identifier should remain the same throughout the life of the system and be retained in audit logs related to system use.

3.0 Information System Responsibility

A designated system owner shall be identified for each system. This person is the primary point of contact (POC) for the system and is responsible for coordinating specific System Development Life Cycle (SDLC) activities as identified in NC DHHS Security Standards, Application Security Standards -

System Development Life Cycle Standard. Additionally, secondary POC's for operation and security shall be appointed. It is important that both the primary and secondary POC's have expert knowledge of the system. These system contacts shall be documented and include the following information:

- Owner: Agency/Division/Office
- Authorizing Official: Agency/Division/Office, name, email, phone number
- Operational Contact: Name, email, phone number
- Security Contact: Name, email, phone number

4.0 Current Information System Operational Status

Divisions or Offices shall indicate the system's operational status using one of the designators below. If more than one status is selected, a list shall be generated by the primary POC detailing which part of the system is covered under each status.

- *Operational* - the system is in production
- *Under Development* - the system is being designed, developed, or implemented
- *Undergoing a major modification* - the system is undergoing a major conversion or transition

If the system is under development or undergoing a major modification, the primary POC shall document any pertinent and verifiable information to ensure that up-front security requirements are considered. Below is a sample table that may be used to document system status:

OPERATIONAL	UNDER DEVELOPMENT	FUTURE MODIFICATION
"Component ID" *if applicable*	"Component ID" *if applicable*	"Component ID" *if applicable*

5.0 Information System Type(s)

Within the Information System Security Plan, Divisions or Offices shall indicate whether a system is a major application or general support system. If the system contains sub applications, the sub applications should be included and described under the appropriate major application. If Divisions and Offices have additional categories of information system types, the template can be modified to include additional categories.

6.0 Information System Description/Purpose

Divisions and Offices shall prepare a brief description of the function and purpose of the system (e.g., health information database, network support for an organization, or business data analysis tool). If the system is a general support system, all applications supported by the general support system shall be listed. It is important to specify if the application is or is not a major application. Where appropriate, unique name/identifiers shall be noted and included. Each application's function, scope, and the information processed shall be included in the documentation.

7.0 Information System Operational Environment

Divisions or Offices shall provide a general description of the system's environmental and technical factors that raise security concerns. One concern may include the use of remote connections or wireless technology. A few of the more common operational environments are listed below, however specific systems in a Division or Office may differ from these and shall be described in the Information System Security Plan as appropriate:

- *Standalone System* - A single, self-contained, or informal computer installation that is used for small-scale applications or individual processing programs not shared across a network.

- *Managed Network or Enterprise System* - Large Department, Division, or Office systems with defined, organized suites of hardware and software configurations usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.

- *Specialized Security* - A specialized security environment containing systems and networks at high risk of attack or data exposure with security taking precedence over functionality. This would be a system that has specialized functionality residing in a vulnerable environment where data protection is considered more critical than data availability.

- *Legacy* - A legacy system often contains older systems or applications that may use outdated or less secure forms of communication. They may also use older software or hardware components that may be difficult to sustain and even more difficult to upgrade or patch.

8.0 Information Systems Interconnection/Sharing

System interconnection must be properly protected to prevent a compromise of all connected systems and the data they store, process, or transmit. It is important for primary and secondary POCs responsible for interconnected systems to know as much as possible regarding vulnerabilities. Divisions or Offices shall document these interconnections as it is essential to selecting the appropriate controls required to mitigate those vulnerabilities. A coordinated and documented operating agreement is needed between the systems sharing data that are owned or operated by different organizations. A few of the common methods that can be used to formalize such an agreement is through a Service Level Agreement (SLA) or Memorandum of Agreement (MOA).

For each interconnection between systems that are owned or operated by different organizations, the following information shall be documented:

- Name of system
- Sharing Divisions or Offices
- Type of interconnection (Internet, Intranet, Dial-Up, etc.)
- Agreements for interconnection
- Certification and accreditation status of system

- Name and title of authorizing official(s)

When systems have numerous interconnections, a table format such as the one below may be a good way to itemize the information:

Component ID/Name	Sharing Organization	Type of Interconnection	Type of Agreement	Date Signed	Cert/Accred. Status	Approving Authority

9.0 Risk Assessment

Divisions and Offices shall follow the process of identifying vulnerabilities and associated risks to confidentiality, integrity, or availability of information systems as outlined in NC DHHS Security Standards, Administrative Security Standards - Information Systems Risk Management Standard. The results of a risk assessment shall be documented in a section of the security plan entitled “Risk Assessment”. The accuracy of the risk assessment is critical to the successful completion of sections 10.0 and 11.0 of this standard.

10.0 Information System Security Categories

For documentation purposes, determining security categories helps organizations identify and implement appropriate security controls for the information systems for which they are responsible. The system vulnerability categories defined below parallel the risk categories used in the overall risk management process outlined in the NC DHHS Security Standards, Administrative Security Standards - Information Systems Risk Management Standard. Example selection guidelines are also included to assist Divisions and Offices in identifying a particular category that is applicable to a specific system.

LOW - The loss of confidentiality, integrity, or availability could be expected to have a minor or limited adverse effect on a Division or Office’s data, information resources, operations, business continuity, or assets. For example, the loss of confidentiality, integrity, or availability might cause a minor degradation in mission capability, temporary inability to perform primary functions, and result in minimal system damage or financial loss.

MODERATE - The loss of confidentiality, integrity, or availability could be expected to have a serious or prolonged adverse effect on a Division or Office’s data, information resources, operations, business continuity, or assets. For example the loss of confidentiality, integrity, or availability might cause a serious, sustained degradation in mission capability, prolonged inability to perform primary functions, result in substantial system damage, or financial loss.

HIGH - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic effect on a Division or Office’s data and information resources, operations, business continuity, or assets. For example, the loss of confidentiality, integrity, or availability cause complete degradation to mission capability, critical inability to perform any operational function, or result in critical system failure or financial loss.

Below is a sample table that may be used for itemizing the security category of a single system or multiple categories of several systems and/or sub-systems:

System/Component	LOW	MODERATE	HIGH
Name/ID	"X" *if Applicable*	"X" *if Applicable*	"X" *if Applicable*

11.0 Information System Security Controls

Divisions and Offices shall identify minimum security controls based on the categories identified in section 10.0 of this standard. The process of selecting the correct security categories and applying the appropriate security controls to achieve adequate security is a multifaceted, risk-based activity that may involve Division or Office management, information technology workforce members, and/or other members of the workforce whose job function may be impacted by a loss of system functionality. All security controls should be reviewed, modified, or tailored as necessary by the system owners and responsible IT staff.

11.1 Types of Security Controls

The three common types of security controls are defined to aid in determining and assigning responsibility for implementation and maintenance.

> ***Management Controls (MC)*****:** These focus on the management of the information system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. Management can and should include both technical and non-technical workforce members – especially those whose operations/job function will be impacted by a loss of system functionality.
>
> ***Operational Controls (OC)*****:** These address security methods focusing on mechanisms primarily implemented and executed by users. These controls are put in place to improve the security of a particular system or group of systems. They often require technical or specialized expertise and often rely upon technical controls as well as management support.
>
> ***Technical Controls (TC)*****:** These focus on security controls that are hardware/software based that IT personnel deploy or that computer systems execute. The controls can provide automated protection for unauthorized access, misuse, facilitate detection of security violations, and support security requirements for applications and data.

Once the security controls have been selected, tailored and the common controls identified, each control shall be described. The description shall contain:

- The security control type and title
- Identify the particular risk addressed by the control
- How the security control is being implemented or planned to be implemented
- Selection guidance used and any alternative considerations
- Indicate if the security control is a common control and who is responsible for its implementation

12.0 Security Control Testing

Once controls are identified, Divisions and Offices shall develop and document a plan to periodically test these controls for security and performance integrity. Periodic testing allows for identification of failures, required patches, necessary upgrades, logical changes to policies, and procedures, etc. Periodic testing is also an important part of incident management by establishing and maintaining a system's operational baseline. The scope, frequency, and responsibility for specific testing shall be identified with each security control identified.

13.0 Risk Management

A comprehensive risk management process is the component of this plan that ensures that all other portions function as planned to identify, rectify, and eliminate risks and vulnerabilities to information systems. Risk management is a formal process that shall be implemented in accordance with NC DHHS Security Standards, Administrative Security Standards - Information Systems Risk Management Standard.

14.0 Security Plan Confidentiality

The information in the Information System Security Plan includes details that describe how an information system is protected against risks. Access to this document must be strictly limited to those with a need to know or maintain this information to ensure that attackers are not provided with an advantage that would simplify their attack. The document shall be appropriately labeled and handled according to its sensitivity.

15.0 Information System Security Plan Maintenance

The dates the Information System Security Plan is completed and subsequently approved shall be documented and a periodic review schedule (recommended quarterly) shall be identified based on the completion date. Identification and contact information for the approval authority shall also be documented. Change management and version control shall be accomplished in accordance with NC DHHS Security Standards, Administrative Security Standards - Information Security Change Management Standard and NC DHHS Security Standards, Application Security Standards - System Development Life Cycle Standard.

References:

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Application Security Policy
  - Information Security Management Policy

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Systems Risk Management Standard
  - Application Security Standards
    - Systems Development Life Cycle Standard